DSK Bescheid vom 20.7.2011, K121.697/0008-DSK/2011 – *Sicherheitspolizeiliche Ermittlung einer IP-Adresse im Chatroom*

1. Ermittelt die Sicherheits- bzw. Kriminalbehörde bei einem Internetdienstleister (hier: Betreiber eines Chatrooms), die von einem Teilnehmer an einem bestimmten Tag benutzte IP-Adresse bei Verdacht auf kinderpornografischem Verhalten, so werden dadurch die berechtigten Geheimhaltungsinteressen des Betroffenen nicht verletzt.
2. § 53 Abs 3a SPG idF BGBl I 114/2007 stellt eine ausreichend deutliche gesetzliche Grundlage iS der Regelung des § 8 Abs 4 Z 1 DSG dar.
2. Dem E-Commerce-Gesetz (ECG) ist keine Intention des Gesetzgebers zu entnehmen, sicherheitsbehördliche Ermittlungsermächtigungen zu beschränken. Darüber hinaus ist § 53 Abs 3a SPG lex posterior zu § 18 Abs 2 ECG und wäre daher letztere Bestimmung auch im Falle eines echten, interpretativen zu lösenden Normenkonflikts nur nachrangig anzuwenden.

Leitsätze verfasst von Dr. *Clemens Thiele*, LL.M.

B E S C H E I D

Die Datenschutzkommission hat unter dem Vorsitz von Dr. SPENLING und in Anwesenheit der Mitglieder Mag. HUTTERER, Dr. SOUHRADA-KIRCHMAYER, Mag. HEILEGGER, Mag. MAITZ-STRASSNIG und Dr. HEISSENBERGER sowie des Schriftführers Mag. SUDA in ihrer Sitzung vom 20. Juli 2011 folgenden Beschluss gefasst:

S p r u c h

Über die Beschwerde des Carl N*** (Beschwerdeführer) aus H***, vertreten durch Dr. Walter D***, Rechtsanwalt in **** H***, vom 17. Jänner 2011 gegen 1. die Bundespolizeidirektion Wien (Erstbeschwerdegegnerin) und 2. das Landespolizeikommando Wien (Zweitbeschwerdegegner) wegen Verletzung im Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten in Folge Ermittlung der vom Beschwerdeführer am 11. November 2009 benutzten IP-Adresse, wird entschieden:
1. Die Beschwerde wird hinsichtlich der Erstbeschwerdegegnerin (Bundespolizeidirektion Wien) abgewiesen.
2. Die Beschwerde wird hinsichtlich des Zweitbeschwerdegegners (Landespolizeikommando Wien, Landeskriminalamt) zurückgewiesen.

Rechtsgrundlagen: §§ 1 Abs 1 und 2, 7 Abs 1, 8 Abs 4 Z 1 und 31 Abs 2 und 7 des Datenschutzgesetzes 2000, BGBl. I Nr 165/1999 idgF, sowie §§ 16 Abs 1 Z 1, Abs 2 Z 1, Abs 3 und Abs 4, 21 Abs 2 und 53 Abs 3a Z 2 und 3 des Sicherheitspolizeigesetzes, BGBl Nr. 566/1991 idF BGBl. I Nr 72/2009.

B e g r ü n d u n g:

A. Vorbringen der Parteien

Der Beschwerdeführer behauptet in seiner am 28. Jänner 2011 bei der Datenschutzkommission eingelangten Beschwerde eine Verletzung im Recht auf Geheimhaltung dadurch, dass die Beschwerdegegner (das Handeln des Zweitbeschwerdegegners sei dabei der Erstbeschwerdegegnerin zuzurechnen) Verkehrsdaten des Internetverkehrs, nämlich die ihm zugewiesene IP-Adresse, ohne richterlichen Beschluss

ermittelt hätten. Anlass sei eine missverständliche Äußerung in einem "sexualbezogenen Phantasiechat" gewesen, die seinen Chatpartner veranlasst habe, eine vermutete strafbare Handlung bei der Polizei zu melden. Zwar sei auf den Sachverhalt § 53 Abs 3a Z 2 SPG anwendbar, es habe jedoch der verfassungsgesetzlich für derartige Anfragen bei den Internet-Providern erforderliche Gerichtsbeschluss gefehlt. Der Betreiber des Chatrooms habe für derartige Auskünfte nämlich erst Verkehrsdaten gemäß § 93 Abs 3 Z 4 TKG 2003, insbesondere Logfiles, auswerten müssen. Eine verfassungskonforme Auslegung von § 53 Abs 3a Z 2 SPG hätte daher zu dem Ergebnis geführt, dass ein solcher Eingriff in das Fernmeldegeheimnis unter Richtervorbehalt stehe. Zur Rechtzeitigkeit der Beschwerde gab der Beschwerdeführer an, am 28. Jänner 2010 anlässlich seiner Einvernahme durch Beamte des Zweitbeschwerdegegners von der Datenermittlung erfahren zu haben.
Die Erstbeschwerdegegnerin (eine eigenständige Befassung des Landespolizeikommandos unterblieb im Hinblick auf die eindeutige Judikatur des Verfassungsgerichtshofs in der Frage der auftraggeberischen Zurechnung derartige Eingriffe) brachte in ihrer Stellungnahme vom 23. Februar 2011 vor, der Beschwerdeführer habe sich in besagtem Chatroom unter Verwendung eines entsprechenden Pseudonyms ("Nickname") als Frau ausgegeben und beim Chatpartner den Eindruck erweckt, sexuelle Handlungen mit Kindern anzubieten. Die daraufhin beim Landeskriminalamt anonym (mit unterdrückter Rufnummer, nicht über den Polizeinotruf, sondern beim SPOC - Single Point of Contact des Ermittlungsdienstes) eingegangene telefonische Meldung habe den Eindruck hinterlassen, ein erfolgter oder noch im Gang befindlicher Angriff auf die Sicherheit Minderjähriger wäre abzuwehren bzw. ein unbekannter Sexualstraftäter auszuforschen. Den daraufhin ermittelnden Beamten sei zunächst durch den Anrufer nur die Webadresse (URL) des Chatrooms bzw. der Nickname des unbekannten Angreifers ("Mama4*H***") bekannt gewesen. Von diesen ausgehend habe man zuerst den Diensteanbieter des Chatrooms und sodann bei diesem die dem User "Mama4*H***" zugeordnete IP-Adresse ermittelt. Die Beamten hätten sich bei diesen Anfragen zu Recht auf § 53 Abs 3a SPG stützen können. Das Gesetz verlange für derartige Anfragen für den hier zu Recht als gegeben angenommenen Zweck der Gefahrenabwehr keinen Gerichtsbeschluss, da solche Ermittlungen noch keinen Eingriff in das verfassungsrechtliche Fernmeldegeheimnis bildeten.
Der Beschwerdeführer replizierte darauf nach Parteiengehör mit der Stellungnahme vom 2. Juli 2011 und brachte ergänzend vor, § 53 Abs 3a SPG habe in eventu auch unter Anwendung von § 18 Abs 2 ECG unangewendet zu bleiben.

B. Beschwerdegegenstand

Auf Grund des Vorbringens des Beschwerdeführers ergibt sich, dass Beschwerdegegenstand die Frage ist, ob die Erstbeschwerdegegnerin (als Sicherheits- bzw. Kriminalpolizeibehörde) am 12. November 2009 berechtigt war, bei Internet-Dienstleistern (Betreiber eines Chatrooms unter der URL http://www.sex***.at) die vom Beschwerdeführer an diesem Tag benutzte IP-Adresse zu ermitteln.

C. Sachverhaltsfeststellungen

Ausgehend vom Beschwerdegegenstand wird der folgende Sachverhalt festgestellt:

Der Beschwerdeführer war mit seinem privaten PC am 11. November 2009 im Internet eingeloggt und benützte die IP-Adresse (Netzadresse seines PC im World Wide Web) **.***.52.157, die ihm von seinem Zugangsprovider, der I-NET*** Webaccess Austria, zugewiesen wurde. Von 14:40 bis jedenfalls gegen 19:40 Uhr war er im Chatroom der Website http://www.sex***.at eingeloggt. Es handelt sich beim Inhaber der URL und

Diensteanbieter um ein Unternehmen, das seinen Usern u.a. Schreibforen und Chatrooms zur Vereinbarung sexueller Kontakte sowie zum Austausch einschlägiger Informationen und Fantasien zur Verfügung stellt. Im Chat erweckte der Beschwerdeführer, der unter dem Pseudonym bzw. Nickname "Mama4*H***" als Frau auftrat, den Eindruck, er wäre bereit, sexuelle Handlungen mit Unmündigen, nämlich "mit 7 - 11jährigen, oder wenn gewünscht auch jünger" zu vermitteln, möglich wäre dies bereits am 14. November 2009. Der unbekannte Chatpartner verstand dies als Angebot verbotener und strafbarer sexueller Handlungen und rief daraufhin selbst oder durch einen, ebenfalls unbekannten, Freund bei der Polizei, nämlich beim SPOC Ermittlungsdienst des Landeskriminalamts Wien, an und ließ den Vorfall melden.

Beweiswürdigung:

Diese Feststellungen beruhen auf den von der Erstbeschwerdegegnerin als Beilage zur Stellungnahme vom 23. Februar 2011, GZ: P3/**568/*/2011, vorgelegten Auszügen aus den Akten des Ermittlungsverfahrens (GZ: zunächst D*/135***/2009, dann B*/086***/2009), insbesondere dem Amtsvermerk über die telefonisch erstattete Meldung vom 11. November 2011 (im Journal, ohne Zahl), dem Abschluss-Bericht an die Staatsanwaltschaft Wien vom 13. November 2009, GZ: B*/086***/2009, sowie den im Internet durchgeführten Abfragen (beginnend mit einer Whois-Suche nach dem Inhaber der URL) und den per Fax eingeholten Auskünfte mehrerer Internet-Provider. Überdies wurde auch die Website http://www.sex***.at eingesehen.
Die Beamten der Erstbeschwerdegegnerin sahen aufgrund der Schilderung eine drohende Gefahr für die Sicherheit Minderjähriger als gegeben. Am 12. November 2009 wurde daher zunächst eine so genannte Whois-Abfrage (Ermittlung der öffentlich zugänglichen Daten des Inhabers einer Domain, das heißt der URL) für http://www.sex***.at vorgenommen (über die Website http://www.utrace.de). Sodann wurde ein Telefax an den in der Whois-Auskunft angegebenen technischen Dienstleister, die (damals nicht mehr bestehende bzw. in der I-NET***-Gruppe aufgegangene) Topweb***-Telekommunikationsdienstleistungs Ges.m.b.H., per Adresse der I-NET*** Austria Ges.m.b.H., abgefertigt. Darin verlangte die Erstbeschwerdegegnerin unter Angabe des Nicknames "Mama4*H***" und der URL www.sex***.at sowie unter Berufung auf § 53 Abs 3a Z 3 SPG Auskunft über "die Daten des Users bzw. dessen IP Adresse". Die I-NET*** Austria Ges.m.b.H. lehnte dies zunächst mit der rechtlichen Begründung ab, es fehle die Angabe einer IP-Adresse und eines Zeitpunkts, zu dem ein Name und eine (Post-) Adresse der IP-Adresse zugeordnet werden könnten. Die ermittelnden Beamten nahmen sodann mit dem Domaininhaber von http://www.sex***.at, bzw. der Firma Net-Performance****Informationssysteme e.U., als technischem Betreiber (Host) des Chatservers Kontakt auf. Von letzterer wurde auf Anfrage gemäß § 53 Abs 3a Z 3 SPG mit Telefax vom 12. November 2009, 17:21 Uhr, die Daten IP-Adresse (**.***.52.157) und Login-Zeitpunkt für den User "Mama4*H***" (2009-11-11 14:40:38 CET) übermittelt. Eine weitere Whois-Abfrage öffentlich zugänglicher Daten ergab, dass der entsprechende Block von IP-Adressen (**.***.7.0 - **.***.129.255) der Firma "I-NET***", das heißt der "I-NET*** Austria", zugewiesen ist. An diese wurde daraufhin am 12. November 2011, 20:14 Uhr, per Telefax eine weitere Anfrage gemäß § 53 Abs 3a Z 3 SPG nach dem Inhaber der IP-Adresse **.***.52.157 zum Zeitpunkt 2009-11-11 14:40:38 CET gerichtet. Die I-NET*** Austria Ges.m.b.H. übermittelte daraufhin die Kunden-Stammdaten Name und Adresse des Beschwerdeführers (Carl N***, E***gasse *21 Tür **, **** H***).

Beweiswürdigung: wie zuletzt.

D. In rechtlicher Hinsicht folgt daraus:

1. anzuwendende Rechtsvorschriften

Die Verfassungsbestimmung § 1 Abs 1 und 2 DSG 2000 lautet samt Überschrift:

"Grundrecht auf Datenschutz

§ 1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.
(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden."
§ 7 Abs 1 DSG 2000 lautet samt Überschrift:
"Zulässigkeit der Verwendung von Daten
§ 7. (1) Daten dürfen nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen."
§ 8 Abs 4 Z 1 DSG 2000 lautet samt Überschrift:

"Schutzwürdige Geheimhaltungsinteressen bei
Verwendung nicht-sensibler Daten

§ 8. (1) [...] (3)
(4) Die Verwendung von Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen verstößt - unbeschadet der Bestimmungen des Abs 2 - nur dann nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen, wenn
1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung solcher Daten besteht oder"

§ 16 SPG lautet samt Überschrift:

"Allgemeine Gefahr; gefährlicher Angriff;

Gefahrenerforschung

§ 16. (1) Eine allgemeine Gefahr besteht

1. bei einem gefährlichen Angriff (Abs 2 und 3)

oder

2. sobald sich drei oder mehr Menschen mit dem Vorsatz verbinden, fortgesetzt gerichtlich strafbare

Handlungen zu begehen (kriminelle Verbindung).

(2) Ein gefährlicher Angriff ist die Bedrohung eines Rechtsgutes durch die rechtswidrige Verwirklichung des Tatbestandes einer gerichtlich strafbaren Handlung, die vorsätzlich begangen und nicht bloß auf Begehren eines Beteiligten verfolgt wird, sofern es sich um einen Straftatbestand

1. nach dem Strafgesetzbuch (StGB), BGBl. Nr. 60/1974, ausgenommen die Tatbestände nach den §§ 278, 278a und 278b StGB, oder

2. nach dem Verbotsgesetz, StGBl. Nr. 13/1945, oder

3. nach dem Fremdenpolizeigesetz 2005 (FPG), BGBl. I Nr. 100, oder

4. nach dem Suchtmittelgesetz (SMG), BGBl. I Nr. 112/1997,

handelt, es sei denn um den Erwerb oder Besitz eines Suchtmittels zum eigenen Gebrauch.

(3) Ein gefährlicher Angriff ist auch ein Verhalten, das darauf abzielt und geeignet ist, eine solche Bedrohung (Abs 2) vorzubereiten, sofern dieses Verhalten in engem zeitlichen Zusammenhang mit der angestrebten Tatbestandsverwirklichung gesetzt wird.

(4) Gefahrenerforschung ist die Feststellung einer Gefahrenquelle und des für die Abwehr einer Gefahr sonst maßgeblichen Sachverhaltes."

§ 21 Abs 1 und 2 SPG lautet samt Überschrift:

"Gefahrenabwehr

§ 21. (1) Den Sicherheitsbehörden obliegt die Abwehr allgemeiner Gefahren.

(2) Die Sicherheitsbehörden haben gefährlichen Angriffen unverzüglich ein Ende zu setzen. Hiefür ist dieses Bundesgesetz auch dann maßgeblich, wenn bereits ein bestimmter Mensch der strafbaren Handlung verdächtig ist."

§ 53 Abs 3a SPG lautet samt Überschrift:

"Zulässigkeit der Verarbeitung

§ 53. (1) [...] (3)

(3a) Die Sicherheitsbehörden sind berechtigt, von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs 3 Z 1 Telekommunikationsgesetz 2003 - TKG 2003,

BGBl. I Nr. 70) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz - ECG, BGBl. I Nr. 152/2001) Auskunft zu verlangen über

1. Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses,

2. Internetprotokolladresse (IP-Adresse) zu einer

bestimmten Nachricht und den Zeitpunkt ihrer

Übermittlung sowie

3. Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war,

wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen und sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen. Die Bezeichnung eines Anschlusses nach Z 1 kann für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer erfolgen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen."

2. rechtliche Schlussfolgerungen

a) Zu den Prozessvoraussetzungen, zeitliches Bestehen des Beschwerderechts:

Der gerügte Eingriff in das Geheimhaltungsrecht (Ermittlung der IP-Adresse) erfolgte am 12. November 2009. Die Beschwerde wurde am Freitag, dem 28. Jänner 2011, um 22:38 Uhr per Telefax an die Geschäftsstelle der Datenschutzkommission gesendet und daher erst am Montag, dem 31. Jänner 2011, als Eingangsstück registriert und als neue Beschwerdesache protokolliert. Da die Datenschutzkommission jedoch keinerlei Beschränkungen gemäß § 13 Abs 2 und 5 AVG (wie: Amtsstunden, Abschaltung der Telekommunikationseinrichtungen außerhalb der Amtsstunden u.ä.) bekanntgemacht hat, und das Faxgerät auch ohne Anwesenheit von Mitarbeiterinnen und Mitarbeitern der Geschäftsstelle technisch empfangsbereit war, ist der rechtlich relevante Zeitpunkt der Beschwerdeerhebung der 28. Jänner 2011. Da der Beschwerdeführer unbestritten und bescheinigt (Beilage zur Beschwerde, Beschuldigtenvernehmung vom 28. Jänner 2010, GZ: B*/086***/2009) erst am 28. Jänner 2010 von dem ihn behauptet beschwerenden Ereignis erfahren hat, erweist sich die Beschwerde als rechtzeitig (innerhalb der Jahresfrist gemäß § 34 Abs 1 erster Fall DSG 2000 erhoben) und damit zulässig.

b) Zu den Prozessvoraussetzungen, fehlende Passivlegitimation des Zweitbeschwerdegegners:

Die hier gegenständliche Ermächtigungsnorm, § 53 Abs 3a SPG, räumt nur den Sicherheitsbehörden besondere Ermittlungsbefugnisse ein. Wie der Beschwerdeführer selbst (Beschwerde, Seite 2) ausführt, war das Handeln des Landeskriminalamts als operativer sicherheitspolizeilicher Einheit der Sicherheitsbehörde zuzurechnen. Gemäß Judikatur des Verfassungsgerichtshofs (Erkenntnis vom 30. November 2005, B 1158/03, RIS) ist es in Angelegenheiten der Sicherheitsverwaltung nicht zulässig, eine interne, organisatorische

Einheit des Wachkörpers (nunmehr: des Korps der Bundespolizei) an Stelle der zuständigen Sicherheitsbehörde als datenschutzrechtlichen Auftraggeber zu behandeln.

Die Beschwerde war daher hinsichtlich des Zweitbeschwerdegegners mangels Passivlegitimation zurückzuweisen.

c) In der Sache selbst:

Die Beschwerde ist hinsichtlich des Handelns der Erstbeschwerdegegnerin (Bundespolizeidirektion Wien als Sicherheitsbehörde) nicht berechtigt.

Zunächst ist auszuführen, dass das von der Datenschutzkommission zu wahrende verfassungsgesetzlich gewährleistete Recht auf Geheimhaltung personenbezogener Daten gemäß § 1 Abs 1 DSG 2000 gemäß Abs 2 leg.cit. - im Gegensatz zum Fernmeldegeheimnis - nicht unter Richtervorbehalt steht.

Der Beschwerdeführer bestreitet jedoch (Beschwerde, Seite 3, unten, wörtlich: "Die Ermittlung der IP-Adresse war ex-ante selbstverständlich nicht nur zulässig sondern auch geboten. Gegenstand dieser Beschwerde ist einzig und allein der Umstand, dass die BGs nicht den gebotenen richterlichen Beschluss eingeholt haben, was unschwer kurzfristig möglich gewesen wäre.") weder das Vorliegen einer konkreten, sicherheitspolizeilich relevanten Gefahrensituation, noch die Möglichkeit, für diesen Zweck einen Grundrechtseingriff vorzunehmen. Er beruft sich allein auf das seiner Ansicht nach verfassungsgesetzlich zwingend vorgegebene Element eines richterlichen Beschlusses, der nicht eingeholt wurde.

In der Beschwerdesache Zl. K121.279 der Datenschutzkommission (Bescheid vom 3. Oktober 2007, GZ: K121.279/0017-DSK/2007, RIS, vom VwGH nach Amtsbeschwerde der Bundesministerin für Inneres mit Erkenntnis vom 27. Mai 2009, Zl. 2007/05/0280; RIS, bestätigt), in dem der Beschwerde stattgegeben wurde, war eine nahezu idente Sachlage gegeben, doch war in jenem Fall noch § 53 SPG in der Fassung vor BGBl. I Nr 114/2007 anzuwenden. Durch Artikel I Z 4 des in letzterem BGBl. kundgemachten Bundesgesetzes wurde § 53 Abs 3a SPG neu gefasst, und wurden die sicherheitspolizeilichen Ermittlungsbefugnisse im Internet-Verkehr deutlich erweitert, sodass gerade derartige Ermittlungen gedeckt sind.

Die Prüfung dieser einfachgesetzlichen Ermächtigungen zu Eingriffen in das Grundrecht auf Datenschutz auf ihre Verfassungskonformität liegt außerhalb der Befugnisse der Datenschutzkommission. Eine vom Beschwerdeführer angeregte verfassungskonforme, einschränkende Auslegung ist auf Grund des klaren Wortlauts und des klaren historischen Zusammenhangs, der diesen Gesetzgebungsakt als "Antwort" auf die oben zitierte Entscheidung der Datenschutzkommission erscheinen lässt (vgl. dazu etwa die vom VfGH wiedergegebene Äußerung der Bundesregierung im Beschluss vom 1. Juli 2009, VfSlg 18.830/2009), nicht möglich. Es war die klare Absicht des Gesetzgebers, derartige Datenermittlungen der Sicherheitsbehörden auch ohne Gerichtsbeschluss zuzulassen. Dabei ist nochmals zu betonen, dass Eingriffe in das Grundrecht auf Datenschutz - im Gegensatz zu solchen in das Fernmeldegeheimnis gemäß Art 10a StGG - nicht unter ausdrücklichem Richtervorbehalt stehen.

In der Rechtsprechung des Obersten Gerichtshofs wird überdies bestritten, dass eine IP-Adresse zu dem unter den Richtervorbehalt fallenden Kern des Fernmeldegeheimnisses zählt:

"Stammdaten unterliegen nicht dem im Art 10a StGG verankerten Grundrecht des Kommunikationsgeheimnisses (§ 93 Abs 1 Satz 1 TKG 2003 e contrario). Selbst bei dynamischen IP-Adressen erfordert die Übermittlung der zugehörigen Stammdaten an ein rite ermittelndes Gericht - der das Grundrecht auf Datenschutz nicht entgegensteht (§ 7 Abs 2 DSG) - keine Feststellung, welche Teilnehmeranschlüsse Ursprung einer Telekommunikation waren (§ 149a Abs 1 Z 1 lit b StPO). Die Erhebung des Namens und der Wohnadresse eines Internetbenutzers, dem eine bestimmte - sei es statische, sei es dynamische - Internetadresse zugewiesen ist oder war, ist unter keinen der Eingriffstatbestände des § 149a Abs 1 Z 1 StPO zu subsumieren; eine planwidrige Gesetzeslücke diesbezüglich ist weder nach dem Regelungsplan des StRÄG 2002 noch des Strafprozessreformgesetzes zu erkennen. Die Stammdaten des Namens und der Wohnanschrift des Inhabers eines bereits individualisierten Teilnehmeranschlusses können gemäß § 103 Abs 4 TKG 2003 formlos bekannt gegeben oder durch formelle Vernehmung einer physischen Person des Access-Providers als Zeugen ermittelt werden, was im Bedarfsfall durch die entsprechenden Zwangsmaßnahmen der Strafprozessordnung durchzusetzen ist." (OGH, 26. 7. 2005, 11 Os 57/05z, RS0120087)

Dies wurde erst jüngst, unter Berücksichtigung der inzwischen wirksamen umfassenden Änderungen der StPO, nochmals vom OGH bestätigt:

"Die Erhebung von Name und Adresse eines Internetbenutzers, dem eine bestimmte - sei es statische, sei es dynamische - Internetadresse zugewiesen ist oder war, ist nicht als Auskunft über Daten einer Nachrichtenübermittlung iSd § 135 Abs 2 StPO zu beurteilen. Sie unterliegt nicht dem Fernmeldegeheimnis des Art 10a StGG, womit sie einer gerichtlichen Bewilligung nicht bedarf." (OGH 13. 4. 2011, EvBl 2011/62, Leitsatz)

Unbestritten ist jedenfalls nur, dass der (Daten-)Inhalt eines Telefonats oder einer Internet-Kommunikation (E-Mail-Inhalte, Chat-Textinhalte u.ä) dem verfassungsrechtlichen Fernmeldegeheimnis unterliegt.

Es steht fest, dass
a) der Beschwerdeführer als User mit seinem PC im Internet eingeloggt war, also bei der ihm zuzurechnenden Handlung (Sendung von Nachrichten in einem Chatroom) eine bestimmte IP-Adresse benutzt hat,
b) der Beschwerdeführer durch eigenes Verhalten zumindest den Anschein einer konkreten, innerhalb der nächsten Tage oder Stunden drohenden Gefahr für die Sicherheit Minderjähriger hervorgerufen hat, von der die Beschwerdegegnerin als Sicherheitsbehörde Kenntnis erlangt hat, und die sie gemäß § 21 Abs 2 SPG abzuwehren verpflichtet war,
c) die die Auskünfte erteilenden Unternehmen unbestritten Diensteanbieter gemäß § 92 Abs 3 Z 1 TKG 2003 bzw. § 3 Z 2 ECG waren, und
d) die Beschwerdegegnerin zur Datenermittlung hinsichtlich der IP-Adresse (der IP-Adresse selbst sowie des Namens und der Adresse des Beschwerdeführers) gemäß § 53 Abs 3a Z 2 und 3 SPG ausdrücklich ermächtigt war.

Damit war der Eingriffstatbestand gemäß der angewendeten Gesetzesbestimmung klar erfüllt. Der Eingriff entspricht auch der generellen Ermächtigung gemäß § 8 Abs 4 Z 1 DSG 2000.

Eine Unverhältnismäßigkeit des Eingriffs bzw. ein überschießendes Handeln oder präsente gelindere Mittel im Vergleich zur Ermittlung der IP-Adresse wurde vom Beschwerdeführer weder behauptet und aufgezeigt, noch haben sich solche Bedenken auf Grundlage des Ergebnisses des Ermittlungsverfahrens ergeben. Die Einholung einer richterlichen Genehmigung wäre dabei kein "gelinderes Mittel" im Sinne eines nach Art und

Eingriffsintensität "anderen" Vorgehens gewesen. Sie hätte lediglich eine nochmalige rechtliche Prüfung durch eine unabhängige richterliche Instanz bewirkt, wobei auch der Beschwerdeführer den inhaltlichen Ausgang dieser Prüfung gar nicht in Zweifel zieht.

Auch aus diesen Blickwinkeln entstehen bei der Datenschutzkommission daher keine Bedenken gegen die Gesetzmäßigkeit des Vorgehens der Sicherheitsbehörde. Auch aus dem Vorbringen des Beschwerdeführers, § 53 Abs 3a SPG habe zu Gunsten von § 18 Abs 2 ECG zurückzutreten bzw. unangewendet zu bleiben, ist für seine Sache nichts zu gewinnen, wiewohl letztere Bestimmung eine richterliche Verfügung vorsieht. Denn § 18 Abs 5 ECG ordnet an: "Sonstige Auskunfts- und Mitwirkungspflichten der Diensteanbieter gegenüber Behörden oder Gerichten bleiben unberührt." Dem ECG ist daher keine Intention des Gesetzgebers zu entnehmen, sicherheitsbehördliche Ermittlungsermächtigungen zu beschränken. Überdies ist § 53 Abs 3a SPG lex posterior zu § 18 Abs 2 ECG (Inkrafttretensdatum: 1. Jänner 2002) und wäre daher letztere Bestimmung auch im Fall eines echten, interpretativ zu lösenden Normenkonflikts nur nachrangig anzuwenden.

Die Beschwerde war daher betreffend die Erstbeschwerdegegnerin gemäß Spruchpunkt 1. als nicht berechtigt abzuweisen.

Anmerkung[*]

I. Das Problem

Der spätere Beschwerdeführer war mit seinem privaten PC am 11.11.2009 im Internet eingeloggt und benutzte die IP-Adresse, die ihn von seinem Zugangsprovider (Access-Provider) zugewiesen wurde. Zu einem ganz bestimmten Zeitpunkt nahm er am Chatroom der Website mit der URL http://www.sex***.at teil. Er führte dabei das Pseudonym bzw. den Nickname „Mama4*H***“. Er trat als Frau auf und erweckte den Eindruck, bereit zu sein, sexuelle Handlungen mit Unmündigen, nämlich „mit Sieben- bis Elfjährigen, oder wenn gewünscht auch jünger“ zu vermitteln; dies binnen drei Tagen. Ein unbekannt gebliebener Chatpartner verstand diese Äußerung als Angebot verbotener und strafbarer sexueller Handlungen iS des § 207a StGB, verständigte daraufhin die Wiener Polizei, nämlich das Sonderkommando gegen Kinderpornographie beim Landeskriminalamt Wien, und meldete den Vorfall. Am 12.11.2009 stellte daraufhin die Bundespolizeidirektion Wien eine Anfrage nach § 53 Abs 3a Z 3 SPG mit Telefax an den Access-Provider um die Daten der ermittelten IP-Adresse zum Login-Zeitpunkt für den User „Mama4*H***“ zu erhalten. Ein gleiches Ersuchen ging an den Domain-Inhaber der aufgerufenen Chatroom-Website und wurden schließlich die Kunden-Stammdaten bestehend aus Name und Adresse des Beschwerdeführers bekannt gegeben.
Im Zuge seiner Einvernahme am 28.1.2010 erfuhr der spätere Beschwerdeführer erstmals von der Ermittlung seiner IP-Adresse und brachte schließlich eine Beschwerde wegen Verletzung seiner berechtigten Geheimhaltungsinteressen gegen die Bundespolizeidirektion und das Landespolizeikommando Wien ein. Die Datenschutzkommission (DSK) hatte sich u.a. mit der Frage zu befassen, ob die belangten Behörden berechtigt waren, bei Internetdienstleistern, insbesondere Betreibern eines Chatrooms, die vom Beschwerdeführer an diesem Tag benutzte IP-Adresse zu ermitteln?

---

* RA Dr. *Clemens Thiele*, LL.M. Tax (GGU),Anwalt.Thiele@eurolawyer.at; Näheres unter http://www.eurolawyer.at.

II. Die Entscheidung der Behörde

Die DSK hielt zunächst zur Rechtzeitigkeit der Beschwerde fest, dass der gerügte Eingriff in das Geheimhaltungsrecht durch Ermittlung der IP-Adresse am 12.11.2009 erfolgte. Die Beschwerde wurde am 28.1.2011 per Telefax an die Geschäftsstelle der DSK übermittelt. Aufgrund der technischen Empfangsbereitschaft und da die DSK nicht den Beschränkungen des § 13 Abs 2 und 5 AVG unterlag, war sohin die Beschwerde rechtzeitig. Dies deshalb, da der Beschwerdeführer erst im Zuge seiner Beschuldigtenvernehmung bei der Polizei am 28.1.2010 von der ermittelten IP-Adresse erfahren hatte. Die Jahresfrist des § 34 Abs 1 erster Fall DSG wurde demnach eingehalten.
Gegenüber dem Landespolizeikommando Wien wurde die Beschwerde mangels Passivlegitimation zurückgewiesen. Dies deshalb, da § 53 Abs 3a SPG lediglich den Sicherheitsbehörden besondere Ermittlungsbefugnisse einräumte und demnach die Handlungen allein der Bundespolizeidirektion Wien als Sicherheitsbehörde zuzurechnen waren.
Die DSK stellte letztlich inhaltlich fest, dass die Bundespolizeidirektion Wien keine berechtigten Geheimhaltungsinteressen des Beschwerdeführers durch die Ermittlung der IP-Adresse verletzt hatte. Nach der auf den Vorfall anwendbaren Fassung des § 53 Abs 3a SPG bestand eine erweiterte sicherheitspolizeiliche Ermittlungsbefugnis im Internet-Verkehr, sodass gerade die Ermittlung der IP-Adresse aufgrund der angenommenen Verdachtslage gedeckt war. Die genannte Gesetzesbestimmung erfüllte die Voraussetzung der generellen Ermächtigung nach § 8 Abs 4 Z 1 DSG. Die Einholung einer richterlichen Genehmigung wäre dabei kein „gelinderes Mittel“ im Sinne eines nach Art und Intensität „anderen“ Vorgehens gewesen. Sie hätte lediglich eine nochmalige rechtliche Prüfung durch eine unabhängige richterliche Instanz bewirkt. Eine Unverhältnismäßigkeit des Eingriffes bzw. ein überschießendes Handeln im Vergleich zur Ermittlung der IP-Adresse bestand ohnehin nicht.

III. Kritische Würdigung und Ausblick:

Da sich der Beschwerdeführer lediglich darauf beschränkt hat, das Fehlen eines „verfassungsgesetzlich zwingend vorgegebenen Elementes eines richterlichen Beschlusses“ vorzubringen, ist das von der DSK gefundene Ergebnis vertretbar. Konnte sich die Sicherheitsbehörde zur Vorläuferbestimmung des § 53 SPG aF für die Abfrage nach der IP-Adresse noch nicht auf eine geeignete gesetzliche Grundlage stützen.[1] Der Gesetzgeber[2] hat im Jahr 2007 rasch reagiert und § 53 SPG im eingangs geschilderten Sinn neu gefasst:

(3a) Die Sicherheitsbehörden sind berechtigt, von Betreibern öffentlicher Telekommunikationsdienste[3] und sonstigen Diensteanbietern[4] Auskunft zu verlangen über

1. Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses,

2. Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung sowie

3. Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war,

wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen und sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen. Die Bezeichnung eines Anschlusses nach Z 1 kann für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer erfolgen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen.“

---

[1] VwGH 27.5.2009, 2007/05/0280, JUS A/5030=jusIT 2009/104, 211 (*Jahnel*).
[2] BGBl I 114/2007.
[3] IS des § 92 Abs 3 Z 1 TKG 2003.
[4] IS des § 3 Z 2 ECG.

Einmal mehr betont die DSK, lediglich für die Prüfung der Einhaltung der gesetzlichen Ermächtigung befugt zu sein. Die Verfassungskonformität derartiger Gesetzesvorbehalte im Hinblick für das Grundrecht auf Datenschutz zu ermessen, liegt „außerhalb der Befugnisse der Datenschutzkommission“. Da Eingriffe in das Grundrecht auf Datenschutz – im Gegensatz zu solchen in das Fernmeldegeheimnis nach Art 10 a StGG – nicht unter ausdrücklichen Richtervorbehalt stehen, geht die Beschwerde daher ins Leere.

Ausblick: Bemerkenswert erscheint die völlig unkritische Übernahme der strafrechtlichen Judikatur, wonach die Erhebung von Name und Adresse eines Internetbenutzers, dem eine bestimmte – sei es statische, sei es dynamische – Internetadresse zugewiesen ist oder war, nicht als Auskunft über Daten einer Nachrichtübermittlung im Sinne des § 135 Abs 2 ZPO beurteilt wird. Nach Auffassung der Strafgerichte unterliegen diese Daten nicht dem Fernmeldegeheimnis des Art 10a StGG, womit sie keiner gerichtlichen Bewilligung bedürfen.[5] Dass die österreichischen Zivilgerichte zur gegenteiligen Auffassung gelangt sind, kann nicht unerwähnt bleiben.[6]

Wie sich die Behördenpraxis angesichts des durch die TKG Novelle zur Vorratsdatenspeicherung[7] neu gefassten Bestimmung des § 99 Abs 5 Z 2 TKG 2003 iVm § 76a StPO entwickelt, bleibt abzuwarten – jedenfalls aber spannend.

IV. Zusammenfassung

Nach nunmehr gefestigter Auffassung der DSK bietet die im Jahr 2007 novellierte Fassung des § 53 Abs 3a SPG eine ausreichende gesetzliche Grundlage iS des § 8 Abs 4 Z 1 DSG, um die sicherheitspolizeiliche Ermittlung einer IP-Adresse eines sich im Chatroom (mutmaßlich) kinderpornografisch äußernden Betroffenen zu ermitteln. Die ermittelten Stammdaten unterlägen nach Ansicht der DSK nicht dem in Art 10a StGG verankerten Grundrecht des Kommunikationsgeheimnisses nach § 93 Abs 1 DKG 2003. Die Bestimmung des § 53 Abs 3a SPG hat nicht gegenüber § 18 Abs 2 ECG zurückzutreten aufgrund der Subsidiaritätsklausel des § 18 Abs 5 ECG.

---

[5] OGH 13.4.2011, 15 Os 172/10y – *Stammdatenherausgabe*, EvBl 2011/62 = JusIT 2011/44, 93 (krit *Karel*) = JBl 2011, 726 (krit *Reindl-Krauskopf*) = MR 2011, 153 (*Hasberger*) = RdW 2011/316, 317 = RZ 2011/23, 252; 26.7.2005, 11 Os 57/05z, 11 Os 58/05x ua – *Auskunftspflicht des Access- Providers*, MR 2005 352 (zust *Daum)* = EvBl 2005/176 = JBl 2006, 130 (krit *Heigenhauser*).

[6] OGH 14.7.2009, 4 Ob 41/09x – *Vermittler III/Media Sentry II*, jusIT 2009/85, 178; dazu *Briem*, Ist der Auskunftsanspruch gegenüber Providern nach § 87b Abs 3 UrhG tot? MR 2011, 55.

[7] BGBl I 27/2011.